NRL Report 7250

Probability-of-Error Considerations for Certain M-Ary Block Codes With Bit-by-Bit Decisions

Noel C. Balthasar and Hugo M. Beck

Communication Systems Branch
Communications Sciences Division

April 26, 1971

NAVAL RESEARCH LABORATORY
Washington, D.C.

Security Classification

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author) Naval Research Laboratory Washington, D.C. 20390	2a. REPORT SECURITY CLASSIFICATION Unclassified 2b. GROUP
3. REPORT TITLE "PROBABILITY-OF-ERROR CONSIDERATIONS FOR CERTAIN M-ARY BLOCK CODES WITH BIT-BY-BIT DECISIONS"	
4. DESCRIPTIVE NOTES (Type of report and inclusive dates) An interim report on the problem.	
5. AUTHOR(S) (First name, middle initial, last name) Noel C. Balthasar and Hugo M. Beck	
6. REPORT DATE April 26, 1971	7a. TOTAL NO. OF PAGES 34 7b. NO. OF REFS
8a. CONTRACT OR GRANT NO. NRL Problem RO101-46 b. PROJECT NO. X-1508, Task H c. d.	9a. ORIGINATOR'S REPORT NUMBER(S) NRL Report 7250 9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)
10. DISTRIBUTION STATEMENT Approved for public release; distribution unlimited.	
11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY Department of the Navy (Naval Electronic Systems Command), Washington, D.C. 20360

13. ABSTRACT

A communication system, which transmits letters from an M-ary source alphabet through an additive white Gaussian noise channel, is considered. The source letters are encoded for transmission using an M-ary block code. Code words are transmitted bit by bit through the channel. The receiver makes hard bit decisions on the received signals, performs, a correlation operation to determine the likeliest transmitted code word and then decodes this word to yield a received letter.

Two types of M-ary block codes are considered. For each type we attempt to derive the probability P_{eB} of a block error, given various values of M (number of block), N (bits per block or block length), and P_{eb} (the probability of a bit error).

The analysis points out the need for investigation of a special-purpose statistical device in order that P_{eB} can be determined for large values of M and N.

DD FORM 1 NOV 65 1473 (PAGE 1)

S/N 0101-807-6801

Security Classification

Security Classification

14. KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Communication theory						
Coding theory						
M-ary Block Code						
Bit-by-Bit Decisions						
Probability p_{eB} of a Block Error						
Correlation						
Equidistributed Random Orthogonal (ERO) Block Code						
Psuedo-orthogonal (PO) Block Code						
Asymptotic Value						
Simulation						
Relative Frequency of a Block Error						
Special-Purpose Statistical Device						
Walsh Functions						
Random Number Generator						

DD FORM 1 NOV 65 1473 (BACK)
(PAGE 2)

Security Classification

CONTENTS

	Page
Abstract	ii
Problem Status	ii
Authorization	ii
M-ARY COMMUNICATION SYSTEM	1
M-ARY BLOCK CODES	1
PROBABILITY P_{eB} OF A BLOCK ERROR	4
Introduction	4
P_{eB} for Binary Block Codes	4
Minimum Distance Considerations for M-ary PO Block Codes	6
P_{eB} for Ternary Block Codes	16
P_{eB} for Quaternary Block Codes	17
Determination of P_{eB} by Simulation	19
AREAS FOR FURTHER INVESTIGATION	22
REFERENCE	22
APPENDIX A - Generating M-ary ERO and M-ary PO Block Codes	23
APPENDIX B - Derivation of P_{eB} Formulas for Ternary ERO and PO Block Codes	25
APPENDIX C - Derivation of P_{eB} Formula for Quaternary ERO Block Codes	28
APPENDIX D - Description of the Digital Computer Simulation of the M-ary Communication System	30

ABSTRACT

A communication system, which transmits letters from an M-ary source alphabet through an additive white Gaussian noise channel, is considered. The source letters are encoded for transmission using an M-ary block code. Code words are transmitted bit by bit through the channel. The receiver makes hard bit decisions on the received signals, performs a correlation operation to determine the likeliest transmitted code word, and then decodes this word to yield a received letter.

Two types of M-ary block codes are considered. For each type we attempt to derive the probability P_{eB} of a block error, given various values of M (number of blocks), N (bits per block, or block length), and P_{eb} (the probability of a bit error).

The analysis points out the need for investigation of a special-purpose statistical device so that P_{eB} can be determined for large values of M and N.

PROBLEM STATUS

This is an interim report: work on the problem is continuing.

AUTHORIZATION

NRL PROBLEM RO1-46
Project X-3297, Task H (formerly X-1508, Task H)

Manuscript submitted January 18, 1971.

PROBABILITY-OF-ERROR CONSIDERATIONS FOR CERTAIN M-ARY BLOCK CODES WITH BIT-BY-BIT DECISIONS

M-ARY COMMUNICATION SYSTEM

The communication system that will be considered in this report is shown in Fig. 1. The source consists of an M-ary alphabet A with letters $a_1, a_2, \ldots, a_M$. Every T seconds the source emits a letter a_i, which the encoder accepts as an input. The encoder has stored an M-ary code consisting of M blocks $B_1, B_2, \ldots, B_M$, each having N bits (zeros and ones), and an encoding function f, which is a one to one mapping of the alphabet A onto the M blocks. For each received letter a_i, the encoder function f determines a corresponding block B_i. Every T seconds the encoder emits a block of N bits $b_{ij} (j = 1, 2, \ldots, N)$ which the transmitter accepts as an input. The transmitter is equipped with a binary signaling set $\{S_0(t), S_1(t)\}$. The transmitter uses the received bits b_{ij} $(j = 1, 2, \ldots, N)$ to determine the signaling sequence $[S_{i1}(t), S_{i2}(t), \ldots, S_{iN}(t)]$. One rule which could be used to determine the N bit signals $S_{ij}(t)$ $(j = 1, \ldots, N)$ is to set $S_{ij}(t) = S_0(t)$ if $b_{ij} = 0$, and $S_{ij}(t) = S_1(t)$ if $b_{ij} = 1$. Every T seconds the transmitter emits a sequence of N bit signals which the channel accepts as an input. The channel adds white Gaussian noise to each bit signal resulting in a sequence of N distorted bit signals $[X_1(t), X_2(t), \ldots, X_N(t)]$. The receiver accepts such a sequence of N distorted bit signals every T seconds, employs a bit-by-bit detection procedure, which depends on the type of binary signaling set utilized at the transmitter, and makes a bit decision d_j on each distorted bit signal $X_j(t)$ $(j = 1, 2, \ldots, N)$. This block D of N bit decisions is the receiver's estimate of the transmitted block B_i. Every T seconds a block of bit decisions D is transferred to the decoder which accepts it as an input. The decoder has stored the same encoding function f and M-ary block code(M by N matrix) which is stored in the encoder. The decoder determines the correlation between the block of bit decisions D and each of the blocks $B_i (i = 1, 2, \ldots, M)$, i.e., $\rho_1, \rho_2, \ldots, \rho_M$ and chooses the maximum (ρ_{MAX}) among these M values.

If $\rho_{MAX} = \rho_j$, then this implies that the bit decision block D is most like block B_j. Using the inverse encoding function f^{-1}, which exists as f is one to one and onto the receiver determines the likeliest transmitted letter, i.e., the letter a_j corresponding to the block B_j. Every T seconds a letter is transferred to the destination.

If $a_j = a_i$, then there was no error in transmitting the letter through our M-ary communication system. If $a_j \neq a_i$, then an error has occurred. An error occurs if the noise causes a sufficient number of errors in the block of bit decisions D so that $\rho_{MAX} \neq \rho_i$. We will assume also that any correlation ties result in an error, i.e., if $\rho_{MAX} = \rho_i = \rho_j$ $(i \neq j)$, then an error has occurred. Further we can allow the encoding function f, the M-ary block code, and the binary signaling set to change for each letter transmitted through our M-ary communication system.

M-ARY BLOCK CODES

The type of M-ary block code utilized at the encoder and decoder is of great importance in minimizing errors. We will consider the error-correcting capabilities of two types of M-ary block codes.

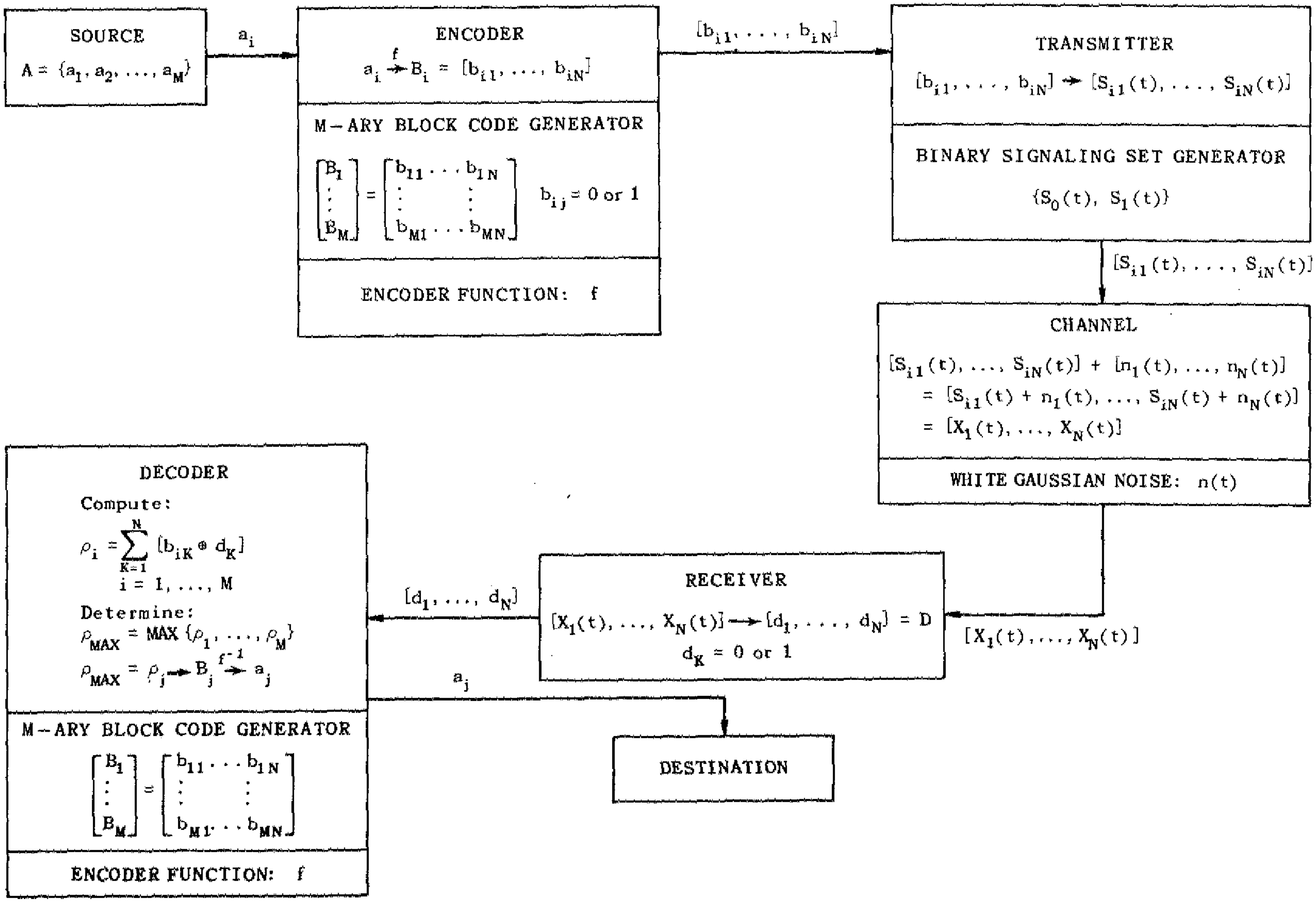


Fig. 1 - Block diagram of M-ary communication system

The first type of M-ary block code is called the M-ary equidistributed random orthogonal (ERO) block code. If N_{xi} and N_{yi} denote the number of zeros and ones, respectively, in block B_i $(i = 1, 2, \ldots, M)$, and ρ_{ij} denotes* the unnormalized correlation between blocks B_i and B_j $(i, j = 1, 2, \ldots, M)$, i.e., the number of bit agreements minus the number of bit disagreements between B_i and B_j, then for an M-ary ERO block code we have, assuming $N/2$ and $N/4$ are integers, the conditions

(i) $N_{xi} = N_{yi} = N/2$ $(i = 1, 2, \ldots, M)$, i.e., there are an equal number of zeros and ones in each block, and

(ii) $\rho_{ij} = \begin{Bmatrix} 0, & i \neq j \\ N, & i = j \end{Bmatrix}$ $(i, j = 1, 2, \ldots, M)$;

That is, between any pair of blocks there are an equal number $(N/2)$ of bit agreements and bit disagreements. Due to conditions (i) and (ii) we must have $M \leq N - 1$.

By definition, the all zeros and all ones blocks do not belong to any M-ary ERO block code.

An example of an M-ary ERO block code for $M = 3$ and $N = 8$ is given by

$$B_1 = [0,\ 1,\ 1,\ 0,\ 1,\ 0,\ 0,\ 1]$$

$$B_2 = [0,\ 1,\ 0,\ 1,\ 0,\ 1,\ 0,\ 1]$$

$$B_3 = [0,\ 0,\ 1,\ 1,\ 1,\ 1,\ 0,\ 0].$$

The second type of M-ary block code is called the M-ary pseudo-orthogonal (PO) block code. An M-ary PO block code is defined in the following manner: the N bits of eaoh block $B_i (i = 1, 2, \ldots, M)$ are determined from N independent Bernoulli trials where, for each trial $k (k = 1, 2, \ldots, N)$, $P(b_{ik} = 0) = P(b_{ik} = 1) = 1/2$. Further, each block is determined in this manner independently of all other blocks. There is no restriction on M for an M-ary PO block code. If N_{xi} and N_{yi} represent the number of zeros and ones, respectively, in block B_i, then for an M-ary PO block code, N_{xi} and N_{yi} are random variables having a binomial distribution $B(n, p)$ with parameters $n = N$ and $p = 1/2$ for each $i = 1, 2, \ldots, M$. Also, if D_{ij} denotes the number of bit disagreements between blocks B_i and B_j, then, for an M-ary PO block code, D_{ij} is a random variable having a binomial distribution $B(n, p)$ with parameters $n = N$ and $p = 1/2$ for all $i, j = 1, 2, \ldots, M$ where $i \neq j$.

An example of an M-ary PO block code for $M = 3$ and $N = 8$ is given by

$$B_1 = [0,\ 1,\ 1,\ 0,\ 0,\ 0,\ 0,\ 1]$$

$$B_2 = [1,\ 1,\ 0,\ 1,\ 1,\ 0,\ 0,\ 1]$$

$$B_3 = [0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 1].$$

---

* $\rho_{ij} = \sum_{k=1}^{N} ([b_{ik} \,\overline{\oplus}\, b_{jk}] - [b_{ik} \oplus b_{jk}])$, where $\oplus$ denotes summation modulo two (exclusive or) and $\overline{\oplus}$ denotes equivalence (not exclusive or).

In this example, $N_{x1} = 5$, $N_{y1} = 3$, $N_{x2} = 3$, $N_{y2} = 5$, $N_{x3} = 6$, $N_{y3} = 2$, $D_{12} = 4$, $D_{13} = 3$, and $D_{23} = 5$.

Methods of generating M-ary ERO and M-ary PO block codes are discussed in App. A. Also in App. A is a discussion of the effect of a bias in the generation of M-ary PO block codes.

PROBABILITY P_{eB} OF A BLOCK ERROR

Introduction

Now we will examine the probability of an error for M-ary ERO and PO block codes. Since each source letter is transmitted in the form of a block of N bits, we will refer to the probability of an error with respect to our M-ary communication system, i.e. the probability that the received letter does not equal the transmitted letter, as the probability of a block error, which will be denoted by P_{eB}. The probability of a block error depends functionally on the type of block code employed (ERO or PO), the number M of blocks in the code, the number of bits N in each block, and the probability of a bit error, which will be denoted by P_{eb}. The probability of a bit error is determined by the type of binary signaling employed at the transmitter and the type of detection employed at the receiver.

P_{eB} for Binary Block Codes

We consider now the determination of P_{eB} for binary ($M = 2$) block codes.

If $B = \{B_1, B_2\}$ is a binary ERO block code, then from condition (ii) of ERO blocks we know, assuming that $N/2$ and $N/4$ are integers, that there are exactly $N/2$ bit agreements and $N/2$ bit disagreements between B_1 and B_2. In determining P_{eB} we need consider only the $N/2$ bit disagreements. This is so because bit decision errors affect the correlation decision only with respect to these bits. Hence, a block error occurs only with $N/4$ or more bit decision errors in the $N/2$ bit disagreements because $N/4$ bit decision errors cause a correlation tie ($\rho_{max} = \rho_1 = \rho_2$), and more than $N/4$ bit decision errors cause a correlation error ($\rho_1 < \rho_2 = \rho_{max}$ if B_1 was transmitted, or $\rho_2 < \rho_1 = \rho_{max}$ if B_2 was transmitted). Hence,

$$P_{eB}\,(\mathrm{ERO},\ 2,\ N,\ P_{eb}) = \sum_{k=N/4}^{N/2} \binom{N/2}{k} P_{eb}^{k} Q_{eb}^{N/2-k}.$$

These curves are given in Fig. 2. Clearly, as P_{eb} tends to zero, $P_{eB}\,(\mathrm{ERO}, 2, N, P_{eb})$ tends to zero. Binary ERO block codes were considered in a previous report (1). The curves given in that report can be used to compare P_{eB} for various types of binary signaling sets and detection procedures.

If $B = \{B_1, B_2\}$ is a binary PO block code, then from the properties of PO blocks we know that the number of bit disagreements between B_1 and B_2 (D_{12}) is a binomially distributed random variable $B(n, p)$ with parameters $n = N$ and $p = 1/2$.

Hence, the probability of d disagreements between B_1 and B_2 is given by

$$P_{D_{12}}(d) = \frac{\binom{N}{d}}{2^N} \quad (d = 0,\ 1,\ \ldots,\ N).$$

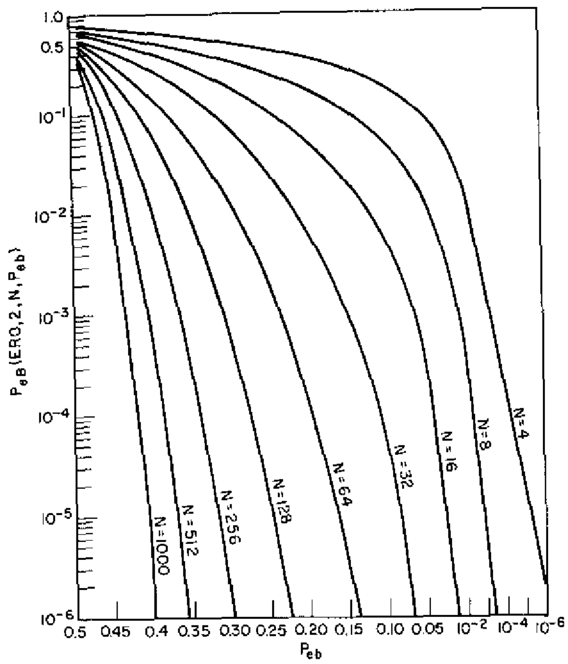


Fig. 2 - Block error probability P_{eB} for a binary (M=2) ERO block code as a function of the bit error probability P_{eb} and the block length N

Now, given d disagreements, a block error occurs if more than $d/2$ (d even) or more than $(d+1)/2$ (d odd) bit decision errors occur. Thus, given d disagreements, the probability of a block error is given by

$$\sum_{k=d/2,\ \text{or}\ (d+1)/2}^{d} \binom{d}{k} P_{eb}^{k} Q_{eb}^{d-k}$$

Hence

$$P_{eB}(\text{PO},\ 2,\ N,\ P_{eb}) = \frac{1}{2^N} + \sum_{d=1}^{N} \frac{\binom{N}{d}}{2^N} \left\{ \sum_{k=d/2,\ \text{or}\ (d+1)/2}^{d} \binom{d}{k} P_{eb}^{k} Q_{eb}^{d-k} \right\}.$$

These curves are given in Fig. 3.

Clearly, as P_{eb} tends to zero, P_{eB} (PO, 2, N, P_{eb}) tends to the value $(1/2)^N$. This value is the probability that there are zero disagreements between blocks B_1 and B_2. If this occurs, then we can have no distinguishable communication of letters since the two blocks which could be transmitted are exactly alike. Thus, independent of any bit errors, a correlation tie will always occur, resulting in a block error.

Suppose now that our binary PO block code has a bias ϵ, i.e., D_{12} is a binomially distributed random variable $B(n, p)$ with $n = N$ and $p = 1/2 - 2\epsilon^2$. Thus, the probability of d disagreement between B_1 and B_2 is given by

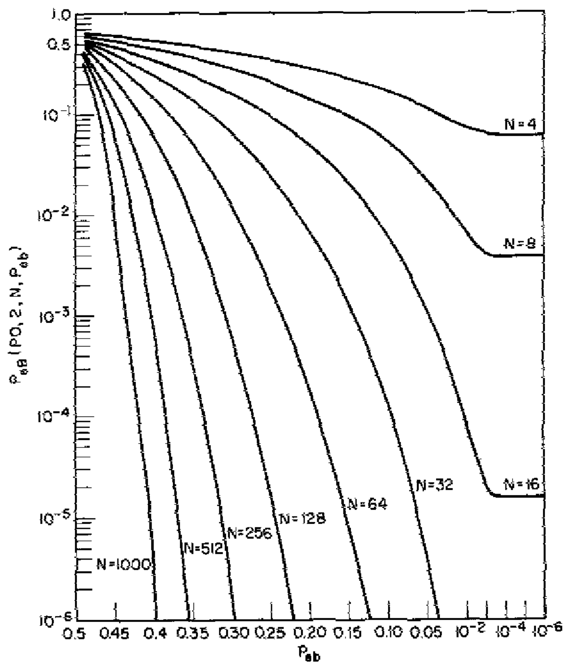


Fig. 3 - Block error probability P_{eB} for a binary (M=2) PO block code as a function of the bit error probability P_{eb} and the block length N

$$P_{D_{12}}(d) = \binom{N}{d} [(1/2) - 2\epsilon^2]^d \; [(1/2) + 2\epsilon^2]^{N-d} \quad (d = 0, 1, \ldots, N).$$

Since the probability of a block error given d disagreements remains unchanged, we have

$$P_{eB}(PO, \epsilon(\text{bias}), 2, N, P_{eb}) =$$

$$[(1/2) + 2\epsilon^2]^N + \sum_{d=1}^{N} \binom{N}{d} [(1/2) - 2\epsilon^2]^d \; [(1/2) + 2\epsilon^2]^{N-d} \left\{ \sum_{k=d/2, \text{ or } (d+1)/2}^{d} \binom{d}{k} P_{eb}^k Q_{eb}^{d-k} \right\}.$$

Clearly, as P_{eb} tends to zero, $P_{eB}(PO, \epsilon(\text{bias}), 2, N, P_{eb})$ tends to the value $[(1/2)+2\epsilon^2]^N$. Note that this value is larger than the corresponding value $[(1/2)]^N$ found in $P_{eB}(PO, 2, N, P_{eb})$. This shows that a bias increases the probability of zero disagreements.

When the $P_{eB}(PO, \epsilon(\text{bias}), 2, N, P_{eb})$ curves were computed, it was found that only for larger values of N and ϵ (say $\epsilon \geq 0.05$) and/or for P_{eb} small could any significant difference be found from the $P_{eB}(PO, 2, N, P_{eb})$ values.

Minimum Distance Considerations for M-ary PO Block Codes

Let us determine the asymptotic value of $P_{eB}(PO, M, N, P_{eb})$ as P_{eb} tends to zero. First, we consider the probability that, given M and N, the minimum number of disagreements between the transmitted block and any other PO block is d_{min}. Let us denote this probability by $P(d_{min}, M, N)$. It is not difficult to show that this probability is given by

$$P(d_{min}, M, N) = \begin{cases} \sum_{k=1}^{M-1} \binom{M-1}{k} \left[\frac{\binom{N}{d_{min}}}{2^N}\right]^k \left[\frac{\left\{\sum_{J=d_{min}+1}^{N} \binom{N}{J}\right\}}{2^N}\right]^{M-1-k}, & d_{min} = 0, 1, \ldots, N-1 \\ \frac{1}{2^{N(M-1)}}, & d_{min} = N \end{cases}.$$

These curves are given for various values of M and N in Fig. 4. Now the asymptotic value of $P_{eB}(PO, M, N, P_{eb})$ as P_{eb} tends to zero is determined by the probability that the number of disagreements between the transmitted block and any of the other PO blocks is zero, i.e., $P(d_{min} = 0, M, N)$. This value is given by

$$P(d_{min} = 0, M, N) = \sum_{k=1}^{M-1} \binom{M-1}{k} \frac{1}{2^{Nk}} \left[\frac{(2^N - 1)}{2^N}\right]^{M-1-k}.$$

Table 1 gives asymptotic values of P_{eB} for various values of M and N.

Now suppose we have an ϵ bias. Then letting

$$X = \binom{N}{d_{min}} [(1/2) - 2\epsilon^2]^{d_{min}} [(1/2) + 2\epsilon^2]^{N-d_{min}}$$

and

$$Y = \sum_{J=d_{min}+1}^{N} \binom{N}{J} [(1/2) - 2\epsilon^2]^J [(1/2) + 2\epsilon^2]^{N-J},$$

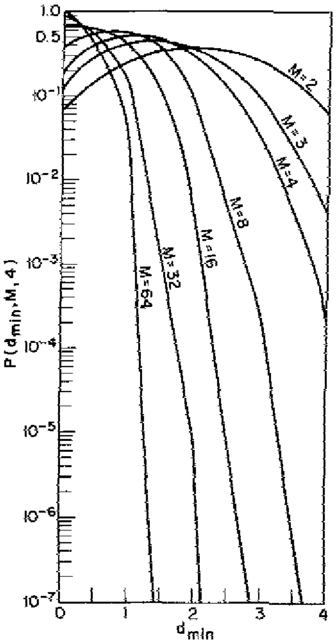
we have

$$P(d_{min}, M, N, \epsilon(\text{bias})) = \begin{cases} \sum_{k=1}^{M-1} \binom{M-1}{k} X^k Y^{M-1-k}, & d_{min} = 0, 1, \ldots, N-1 \\ [(1/2) - 2\epsilon^2]^{N(M-1)}, & d_{min} = N \end{cases}$$

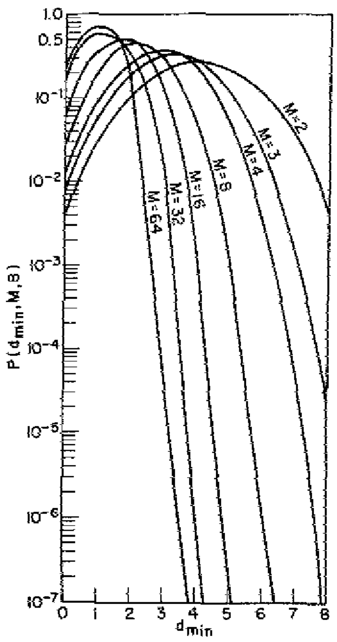
and

$$P(d_{min} = 0, M, N, \epsilon(\text{bias})) = \sum_{k=1}^{M-1} \binom{M-1}{k} [(1/2) + 2\epsilon^2]^{Nk} \left\{1 - [(1/2) + 2\epsilon^2]^N\right\}^{M-1-k}.$$

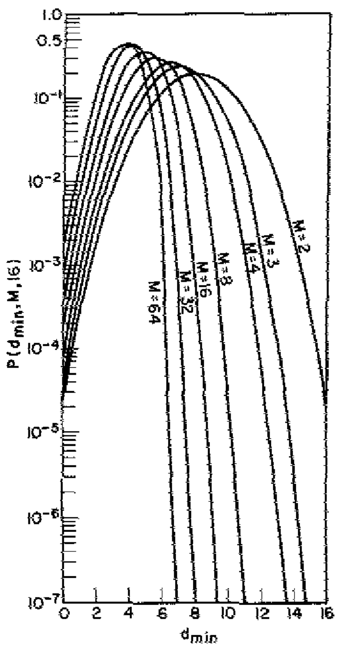
Tables 2 to 6 give values for $P(d_{min} = 0, M, N, \epsilon(\text{bias})$ for $\epsilon = 0.001, 0.01, 0.05, 0.1$, and 0.15, and various values of M and N. Comparing these values with the values for $P(d_{min} = 0, M, N$, one can clearly see the effect of a bias on the asymptotic values for an M-ary PO block code.



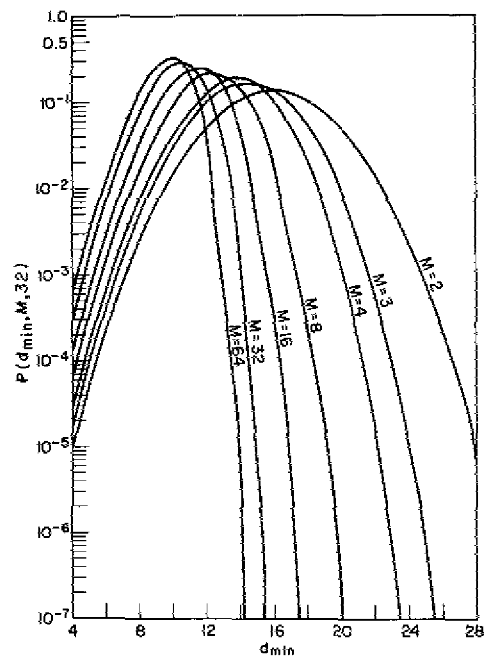
(N = 4)



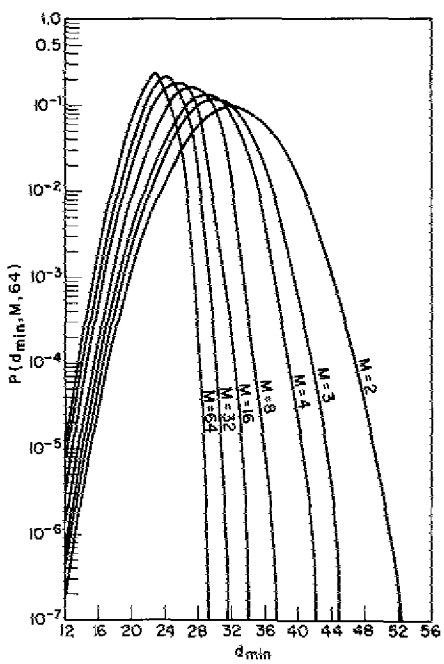
(N = 8)



(N = 16)



(N = 32)



(N = 64)

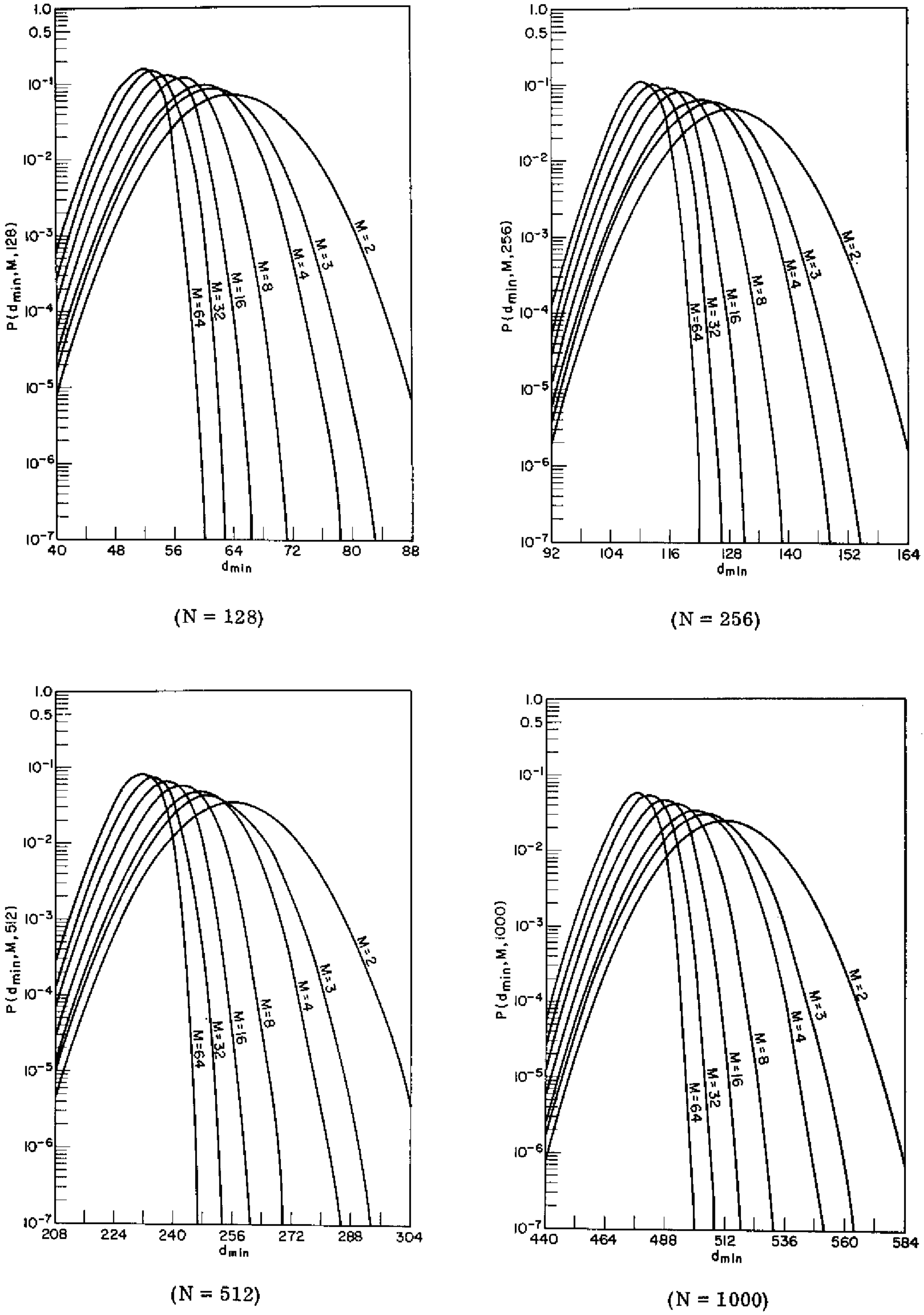


Fig. 4 - Probability P that, for the indicated values of M and N, the minimum number of bit disagreements between the transmitted block and any other PO block is d_{min}. The curves are grouped according to the choice of N (number of bits in each block M).

Table 1

Asymptotic Values of P_{eB} (PO, ϵ, M, N, P_{eb}) as $P_{eb} \to 0$ with $\epsilon = 0$.

N \ M	2	3	4	8	16	32	64
4	$6.25*10^{-2}$	$1.21094*10^{-1}$	$1.76025*10^{-1}$	$3.63499*10^{-1}$	$6.20188*10^{-1}$	$8.64759*10^{-1}$	$9.82853*10^{-1}$
8	$3.90625*10^{-3}$	$7.79724*10^{-3}$	$1.16730*10^{-2}$	$2.70254*10^{-2}$	$5.70184*10^{-2}$	$1.14259*10^{-1}$	$2.18528*10^{-1}$
16	$1.52588*10^{-5}$	$3.05173*10^{-5}$	$4.57757*10^{-5}$	$1.06807*10^{-4}$	$2.28857*10^{-4}$	$4.72914*10^{-4}$	$9.60849*10^{-4}$
32	$2.32831*10^{-10}$	$4.65661*10^{-10}$	$6.98492*10^{-10}$	$1.62981*10^{-9}$	$3.49246*10^{-9}$	$7.21775*10^{-9}$	$1.46683*10^{-8}$
64	$5.42101*10^{-20}$	$1.08420*10^{-19}$	$1.62630*10^{-19}$	$3.79481*10^{-19}$	$8.13152*10^{-19}$	$1.68051*10^{-18}$	$3.41524*10^{-18}$
128	$2.93874*10^{-39}$	$5.87747*10^{-39}$	$8.81621*10^{-39}$	$2.05712*10^{-38}$	$4.40810*10^{-38}$	$9.11008*10^{-38}$	$1.85140*10^{-37}$
256	$8.63617*10^{-78}$	$1.72723*10^{-77}$	$2.59085*10^{-77}$	$6.04532*10^{-77}$	$1.29543*10^{-76}$	$2.67721*10^{-76}$	$5.44079*10^{-76}$
512	$7.45834*10^{-155}$	$1.49167*10^{-154}$	$2.23750*10^{-154}$	$5.22084*10^{-154}$	$1.11875*10^{-153}$	$2.31209*10^{-153}$	$4.69875*10^{-153}$
1000	$9.33264*10^{-302}$	$1.86653*10^{-301}$	$2.79979*10^{-301}$	$6.53285*10^{-301}$	$1.39990*10^{-300}$	$2.89312*10^{-300}$	$5.87956*10^{-300}$

Table 2

Asymptotic Values of P_{eB} (PO, ϵ, M, N, P_{eB}) as $P_{eb} \rightarrow 0$ with $\epsilon = 0.001$.

N \ M	2	3	4	8	16	32	64
4	$6.25010*10^{-2}$	$1.21096*10^{-1}$	$1.76028*10^{-1}$	$3.63504*10^{-1}$	$6.20194*10^{-1}$	$8.64763*10^{-1}$	$9.82854*10^{-1}$
8	$3.90638*10^{-3}$	$7.79749*10^{-3}$	$1.16734*10^{-2}$	$2.70262*10^{-2}$	$5.70202*10^{-2}$	$1.14263*10^{-1}$	$2.18534*10^{-1}$
16	$1.52598*10^{-5}$	$3.05193*10^{-5}$	$4.57786*10^{-5}$	$1.06813*10^{-4}$	$2.28872*10^{-4}$	$4.72944*10^{-4}$	$9.60911*10^{-4}$
32	$2.32860*10^{-10}$	$4.65721*10^{-10}$	$6.98581*10^{-10}$	$1.63002*10^{-9}$	$3.49291*10^{-9}$	$7.21867*10^{-9}$	$1.46702*10^{-8}$
64	$5.42240*10^{-20}$	$1.08448*10^{-19}$	$1.62672*10^{-19}$	$3.79568*10^{-19}$	$8.13360*10^{-19}$	$1.68094*10^{-18}$	$3.41611*10^{-18}$
128	$2.94024*10^{-39}$	$5.88048*10^{-39}$	$8.82072*10^{-39}$	$2.05817*10^{-38}$	$4.41036*10^{-38}$	$9.11475*10^{-38}$	$1.85235*10^{-37}$
256	$8.64502*10^{-78}$	$1.72900*10^{-77}$	$2.59350*10^{-77}$	$6.05151*10^{-77}$	$1.29675*10^{-76}$	$2.67995*10^{-76}$	$5.44636*10^{-76}$
512	$7.47363*10^{-155}$	$1.49473*10^{-154}$	$2.24209*10^{-154}$	$5.23154*10^{-154}$	$1.12104*10^{-153}$	$2.31683*10^{-153}$	$4.70839*10^{-153}$
1000	$9.37004*10^{-302}$	$1.87401*10^{-301}$	$2.81101*10^{-301}$	$6.55903*10^{-301}$	$1.40551*10^{-300}$	$2.90471*10^{-300}$	$5.90312*10^{-300}$

Table 3

Asymptotic Values of P_{eB} (PO, ϵ, M, N, P_{eb}) as $P_{eB} \to 0$ with $\epsilon = 0.01$.

N \ M	2	3	4	8	16	32	64
4	$6.26001*10^{-2}$	$1.21281*10^{-1}$	$1.76289*10^{-1}$	$3.63975*10^{-1}$	$6.20795*10^{-1}$	$8.65205*10^{-1}$	$9.82968*10^{-1}$
8	$3.91877*10^{-3}$	$7.82218*10^{-3}$	$1.17103*10^{-2}$	$2.71110*10^{-2}$	$5.71961*10^{-2}$	$1.14604*10^{-1}$	$2.19146*10^{-1}$
16	$1.53567*10^{-5}$	$3.07132*10^{-5}$	$4.60695*10^{-5}$	$1.07492*10^{-4}$	$2.30326*10^{-4}$	$4.75949*10^{-4}$	$9.67014*10^{-4}$
32	$2.35829*10^{-10}$	$4.71659*10^{-10}$	$7.07488*10^{-10}$	$1.65081*10^{-9}$	$3.53744*10^{-9}$	$7.31071*10^{-9}$	$1.48573*10^{-8}$
64	$5.56155*10^{-20}$	$1.11231*10^{-19}$	$1.66847*10^{-19}$	$3.89309*10^{-19}$	$8.34233*10^{-19}$	$1.72408*10^{-18}$	$3.50378*10^{-18}$
128	$3.09309*10^{-39}$	$6.18617*10^{-39}$	$9.27926*10^{-39}$	$2.16516*10^{-38}$	$4.63963*10^{-38}$	$9.58857*10^{-38}$	$1.94864*10^{-37}$
256	$9.56718*10^{-78}$	$1.91344*10^{-77}$	$2.87015*10^{-77}$	$6.69703*10^{-77}$	$1.43508*10^{-76}$	$2.96583*10^{-76}$	$6.02732*10^{-76}$
512	$9.15309*10^{-155}$	$1.83062*10^{-154}$	$2.74593*10^{-154}$	$6.40717*10^{-154}$	$1.37296*10^{-153}$	$2.83746*10^{-153}$	$5.76645*10^{-153}$
1000	$1.39215*10^{-301}$	$2.78431*10^{-301}$	$4.17646*10^{-301}$	$9.74508*10^{-301}$	$2.08823*10^{-300}$	$4.31568*10^{-300}$	$8.77057*10^{-300}$

Table 4

Asymptotic Values of P_{eB} (PO, ϵ, M, N, P_{eb}) as $P_{eb} \rightarrow 0$ with $\epsilon = 0.05$.

N \ M	2	3	4	8	16	32	64
4	$6.50378*10^{-2}$	$1.25846*10^{-1}$	$1.82699*10^{-1}$	$3.75462*10^{-1}$	$6.35321*10^{-1}$	$8.75658*10^{-1}$	$9.85545*10^{-1}$
8	$4.22991*10^{-3}$	$8.44193*10^{-3}$	$1.26361*10^{-2}$	$2.92363*10^{-2}$	$6.16040*10^{-2}$	$1.23138*10^{-1}$	$2.34365*10^{-1}$
16	$1.78921*10^{-5}$	$3.57839*10^{-5}$	$5.36754*10^{-5}$	$1.25238*10^{-4}$	$2.68348*10^{-4}$	$5.54507*10^{-4}$	$1.12658*10^{-3}$
32	$3.20128*10^{-10}$	$6.40257*10^{-10}$	$9.60385*10^{-10}$	$2.24090*10^{-9}$	$4.80192*10^{-9}$	$9.92398*10^{-9}$	$2.01681*10^{-8}$
64	$1.02482*10^{-19}$	$2.04964*10^{-19}$	$3.07446*10^{-19}$	$7.17375*10^{-19}$	$1.53723*10^{-18}$	$3.17695*10^{-18}$	$6.45638*10^{-18}$
128	$1.05026*10^{-38}$	$2.10052*10^{-38}$	$3.15078*10^{-38}$	$7.35181*10^{-38}$	$1.57539*10^{-37}$	$3.25580*10^{-37}$	$6.61663*10^{-37}$
256	$1.10304*10^{-76}$	$2.20609*10^{-76}$	$3.30913*10^{-76}$	$7.72131*10^{-76}$	$1.65457*10^{-75}$	$3.41944*10^{-75}$	$6.94918*10^{-75}$
512	$1.21671*10^{-152}$	$2.43341*10^{-152}$	$3.65012*10^{-152}$	$8.51694*10^{-152}$	$1.82506*10^{-151}$	$3.77179*10^{-151}$	$7.66525*10^{-151}$
1000	$1.95604*10^{-297}$	$3.91208*10^{-297}$	$5.86813*10^{-297}$	$1.36923*10^{-296}$	$2.93406*10^{-296}$	$6.06373*10^{-296}$	$1.23231*10^{-295}$

Table 5

Asymptotic Values of P_{eB} (PO, ϵ, M, N, P_{eb}) as $P_{eb} \rightarrow 0$ with $\epsilon = 0.10$.

N \ M	2	3	4	8	16	32	64
4	$7.31162*10^{-2}$	$1.40886*10^{-1}$	$2.03701*10^{-1}$	$4.12271*10^{-1}$	$6.79831*10^{-1}$	$9.04987*10^{-1}$	$9.91633*10^{-1}$
8	$5.34597*10^{-3}$	$1.06634*10^{-2}$	$1.59523*10^{-2}$	$3.68270*10^{-2}$	$7.72572*10^{-2}$	$1.53098*10^{-1}$	$2.86591*10^{-1}$
16	$2.85794*10^{-5}$	$5.71580*10^{-5}$	$8.57358*10^{-5}$	$2.00039*10^{-4}$	$4.28606*10^{-4}$	$8.85583*10^{-4}$	$1.79891*10^{-3}$
32	$8.16784*10^{-10}$	$1.63357*10^{-9}$	$2.45035*10^{-9}$	$5.71749*10^{-9}$	$1.22518*10^{-8}$	$2.53203*10^{-8}$	$5.14574*10^{-8}$
64	$6.67135*10^{-19}$	$1.33427*10^{-18}$	$2.00141*10^{-18}$	$4.66995*10^{-18}$	$1.00070*10^{-17}$	$2.06812*10^{-17}$	$4.20295*10^{-17}$
128	$4.45070*10^{-37}$	$8.90139*10^{-37}$	$1.33521*10^{-36}$	$3.11549*10^{-36}$	$6.67604*10^{-36}$	$1.37972*10^{-35}$	$2.80394*10^{-35}$
256	$1.98087*10^{-73}$	$3.96174*10^{-73}$	$5.94261*10^{-73}$	$1.38661*10^{-72}$	$2.97131*10^{-72}$	$6.14070*10^{-72}$	$1.24795*10^{-71}$
512	$3.92385*10^{-146}$	$7.84769*10^{-146}$	$1.17715*10^{-145}$	$2.74669*10^{-145}$	$5.88577*10^{-145}$	$1.21639*10^{-144}$	$2.47202*10^{-144}$
1000	$1.00773*10^{-284}$	$2.01546*10^{-284}$	$3.02319*10^{-284}$	$7.05410*10^{-284}$	$1.51159*10^{-283}$	$3.12396*10^{-283}$	$6.34869*10^{-283}$

Table 6

Asymptotic Values of P_{eB} $(PO, \epsilon, M, N, P_{eb})$ as $P_{eb} \to 0$ with $\epsilon = 0.15$.

N \ M	2	3	4	8	16	32	64
4	$8.82239*10^{-2}$	$1.68664*10^{-1}$	$2.42008*10^{-1}$	$4.76137*10^{-1}$	$7.49779*10^{-1}$	$9.42913*10^{-1}$	$9.97029*10^{-1}$
8	$7.78345*10^{-3}$	$1.55063*10^{-2}$	$2.31691*10^{-2}$	$5.32283*10^{-2}$	$1.10600*10^{-1}$	$2.15125*10^{-1}$	$3.88766*10^{-1}$
16	$6.05821*10^{-5}$	$1.21160*10^{-4}$	$1.81735*10^{-4}$	$4.23997*10^{-4}$	$9.08346*10^{-4}$	$1.87634*10^{-3}$	$3.80951*10^{-3}$
32	$3.67019*10^{-9}$	$7.34037*10^{-9}$	$1.10106*10^{-8}$	$2.56913*10^{-8}$	$5.50528*10^{-8}$	$1.13776*10^{-7}$	$2.31222*10^{-7}$
64	$1.34703*10^{-17}$	$2.69405*10^{-17}$	$4.04108*10^{-17}$	$9.42919*10^{-17}$	$2.02054*10^{-16}$	$4.17578*10^{-16}$	$8.48627*10^{-16}$
128	$1.81448*10^{-34}$	$3.62960*10^{-34}$	$5.44344*10^{-34}$	$1.27014*10^{-33}$	$2.72172*10^{-33}$	$5.62489*10^{-33}$	$1.14312*10^{-32}$
256	$3.29234*10^{-68}$	$6.58468*10^{-68}$	$9.87702*10^{-68}$	$2.30464*10^{-67}$	$4.93851*10^{-67}$	$1.02063*10^{-66}$	$2.07417*10^{-66}$
512	$1.08395*10^{-135}$	$2.16790*10^{-135}$	$3.25185*10^{-135}$	$7.58765*10^{-135}$	$1.62592*10^{-134}$	$3.36024*10^{-134}$	$6.82888*10^{-134}$
1000	$2.49174*10^{-264}$	$4.98347*10^{-264}$	$7.47521*10^{-264}$	$1.74422*10^{-263}$	$3.73761*10^{-263}$	$7.72438*10^{-263}$	$1.56979*10^{-262}$

In order to be able to compare $P(d_{min}, M, N, \epsilon(\text{bias}))$ and $P(d_{min}, M, N)$, we computed $P(d_{min}, M, N, \epsilon(\text{bias}))$ for various values of M and N with $\epsilon = 0.01$ and 0.1. It was found that given M and N, a value of d_{min} (say d), depending on M, N, and ϵ, could be determined such that for $0 \le d_{min} < d$, $P(d_{min}, M, N, \epsilon(\text{bias})) > P(d_{min}, M, N)$, and for $d \le d_{min} \le N$, $P(d_{min}, M, N) > P(d_{min}, M, N, \epsilon(\text{bias}))$. When $M = 2$, $d = N/2$ (independent of ϵ). It was found that for $\epsilon = 0.1$, the value d was given by that value of d_{min} which maximized the value $P(d_{min}, M, N)$. For $\epsilon = 0.01$, the corresponding value of d was slightly larger than the value of d for $\epsilon = 0.1$.

P_{eB} for Ternary Block Codes

Next we examine P_{eB} for ternary ($M = 3$) block codes. In App. B the formula for P_{eB} is derived for both ternary ERO and PO block codes.

For a ternary ERO block code we have, assuming $N/4$ is an integer,

$$P_{eB}(\text{ERO}, 3, N, P_{eb}) = \sum_{J=0}^{N/4-1} \binom{N/4}{J} P_{eb}^{J} Q_{eb}^{(N/4)-J} \left\{ \left(\sum_{k=(N/4)-J}^{N/4} \binom{N/4}{k} P_{eb}^{k} Q_{eb}^{(N/4)-k} \right) S \right\}$$

where

$$S = 1 + \sum_{L=0}^{(N/4)-J-1} \binom{N/4}{L} P_{eb}^{L} Q_{eb}^{(N/4)-L}.$$

These curves are given in Fig. 5. Clearly, as P_{eb} tends to zero, $P_{eB}(\text{ERO}, 3, N, P_{eb})$ tends to zero.

For a ternary PO block code we have, using the definitions of D_{12}, D_{13}, d_{min}, d_{max}, d_0, d_1, and d_x given in App. B,

$$P_{eB}(\text{PO}, 3, N, P_{eb}) = \frac{(2^{N+1}-1)}{2^{2N}} + \sum_{D_{12}=1}^{N} \sum_{D_{13}=1}^{N} \left[\frac{\binom{N}{D_{12}}\binom{N}{D_{13}}}{2^{2N}} \right] \left\{ \sum_{d_0=0}^{d_{min}} \left[\frac{\binom{d_{min}}{d_0}\binom{N-d_{min}}{d_{max}-d_0}}{\binom{N}{d_{max}}} \right] R \right\}$$

where

$$R = \sum_{e=0}^{d_i-1} \binom{d_0}{e} P_{eb}^{e} Q_{eb}^{d_0-e} \left\{ \sum_{J=d_i-e}^{d_{min}-d_0} \binom{d_{min}-d_0}{J} P_{eb}^{J} Q_{eb}^{d_{min}-d_0-J} + \left[Z \sum_{k=0}^{d_i-e-1} \binom{d_{min}-d_0}{k} P_{eb}^{k} Q_{eb}^{d_{min}-d_0-k} \right] \right\}$$

$$+ \sum_{e=d_i}^{d_0} \binom{d_0}{e} P_{eb}^{e} Q_{eb}^{d_0-e}$$

with

$$Z = \sum_{L=d_x-e}^{d_x-d_0} \binom{d_{max}-d_0}{L} P_{eb}^{L} Q_{eb}^{d_{max}-d_0-L}.$$

These curves are given in Fig. 6 for $N = 4$, 8, 16, 32, 64, and 128. The approximations described in App. B were used in computing the curves for $N = 32$, 64, and 128. Due to the lengthy computation time, $N = 128$ was the largest value for which the approximation was computed. Clearly, as P_{eb} tends to zero, $P_{eB}(\text{PO}, 3, N, P_{eb})$ tends to the asymptotic value $[2^{N+1} - 1]/2^{2N}$, which is the value of $P(d_{min}=0, 3, N)$.

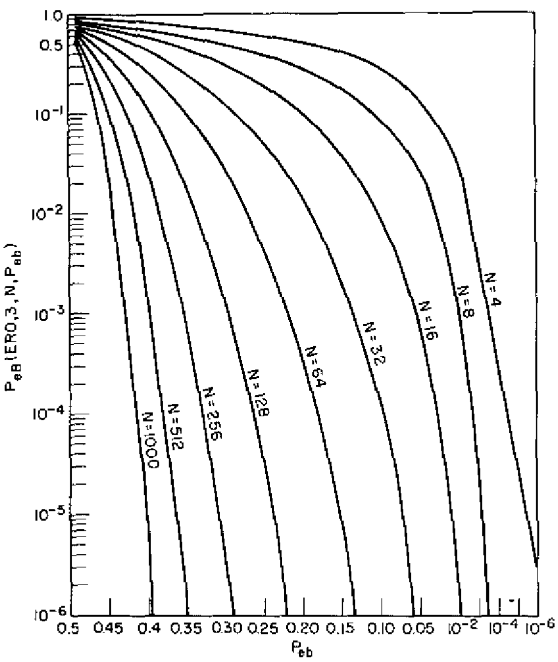


Fig. 5 - Block error probability P_{eB} for a ternary (M=3) ERO block code as a function of the bit error probability P_{eb} and the block length N

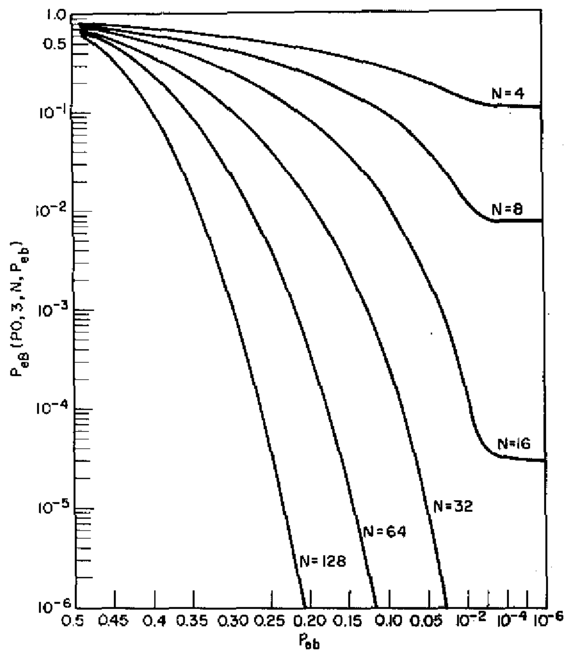


Fig. 6 - Block error probability P_{eB} for a ternary (M=3) PO block code as a function of the bit error probability P_{eb} and the block length N

P_{eB} for Quaternary Block Codes

Now we examine P_{eB} for quaternary (M = 4) block codes. In App. C the formula for P_{eB} is derived for quaternary ERO block codes. We have, using the definitions of e_1, e_{12}, e_{13}, and e_{14} given in App. C, and assuming that $N/8$ is an integer,

$$P_{eB}(\mathrm{ERO}, 4, N, P_{eb}) = \sum_{e_1=0}^{N/8} \sum_{e_{12}=0}^{N/8} \sum_{e_{13}=0}^{N/8} \sum_{e_{14}=0}^{N/8} \binom{N/8}{e_1}\binom{N/8}{e_{12}}\binom{N/8}{e_{13}}\binom{N/8}{e_{14}} P_{eb}^{X} Q_{eb}^{(N/2)-X} R$$

where

$$X = e_1 + e_{12} + e_{13} + e_{14}$$

and

$$R = \begin{cases} 1, & \text{if } e_1 + e_{13} + e_{14} \geq N/4, \text{ or } e_1 + e_{12} + e_{14} \geq N/4, \text{ or } e_1 + e_{12} + e_{13} \geq N/4 \\ T, & \text{otherwise} \end{cases}$$

with

$$T = A + (1-A)\,B + (1-A)\,(1-B)\,C$$

and

$$A = \sum_{e_{134}=(N/4)-(e_1+e_{13}+e_{14})}^{N/8} \binom{N/8}{e_{134}} P_{eb}^{e_{134}}\, Q_{eb}^{(N/8)-e_{134}}$$

$$B = \sum_{e_{124}=(N/4)-(e_1+e_{12}+e_{14})}^{N/8} \binom{N/8}{e_{124}} P_{eb}^{e_{124}} Q_{eb}^{(N/8)-e_{124}}$$

$$C = \sum_{e_{123}=(N/4)-(e_1+e_{12}+e_{13})}^{N/8} \binom{N/8}{e_{123}} P_{eb}^{e_{123}} Q_{eb}^{(N/8)-e_{123}}.$$

These curves are given in Fig. 7 for $N = 8$, 16, 32, 64, and 128. Clearly, as P_{eb} tends to zero, P_{eB} (ERO, 4, N, P_{eb}) tends to zero. Due to the considerations mentioned in App. C concerning the computational problems encountered in determining P_{eB} (ERO, 4, N, P_{eb}), the determination and computation of the exact formula for P_{eB}(ERO, M, N, P_{eb}) when $M > 4$ is clearly not feasible.

Next let us consider the determination of P_{eB} for a quaternary PO block code.

To determine P_{eB}(PO, 4, N, P_{eb}), one must be able to determine $P(d_1, d_2, d_3)$, and P_{eB} given d_1, d_2, and d_3 (symbolically, $P_{eB} | d_1, d_2, d_3$), where d_1, d_2, and d_3 represent the distances between the transmitted block and $M - 1 = 3$ nontransmitted blocks. If this is possible, then we have

$$P_{eB}(PO, 4, N, P_{eb}) = \sum_{d_1=0}^{N} \sum_{d_2=0}^{N} \sum_{d_3=0}^{N} P(d_1, d_2, d_3)\ P_{eB} | d_1, d_2, d_3 .$$

Hence, in determining P_{eB} for a quaternary PO block code, a triple sum arises. The computational difficulties in evaluating this expression are due to the problems

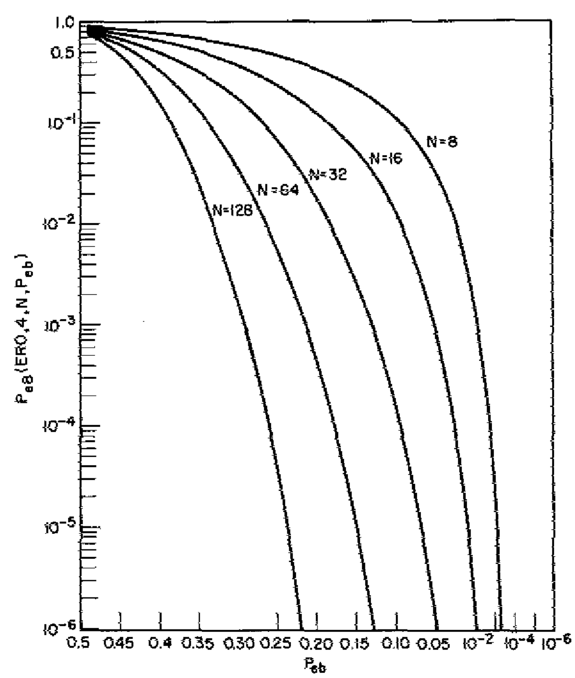


Fig. 7 - Block error probability P_{eB} for a quarternary ($M=4$) ERO block code as a function of the bit error probability and the block length N

involved in the evaluation of $P_{eB}|d_1, d_2, d_3$ since, due to the independence of the blocks, we have

$$P(d_1, d_2, d_3) = P(d_1)\,P(d_2)\,P(d_3) = \frac{\binom{N}{d_1}\binom{N}{d_2}\binom{N}{d_3}}{2^{3N}},$$

or in the case of an ϵ bias

$$P(d_1, d_2, d_3) = \binom{N}{d_1}\binom{N}{d_2}\binom{N}{d_3}\left[(1/2) - 2\epsilon^2\right]^{(d_1+d_2+d_3)}\left[(1/2) + 2\epsilon^2\right]^{3N-(d_1+d_2+d_3)}.$$

Even the use of $P(d_{min}, 4, N)$ in the place of $P(d_1, d_2, d_3)$, which reduces the triple sum to a single sum, does not solve the problem of computing $P_{eB}|d_1, d_2, d_3$ since we then have to compute $P_{eB}|d_{min}$, which involves the additional problem of choosing values for d_2 and d_3, if say $d_1 = d_{min}$, and hence introduces considerable error. Due to these considerations the direct calculation of $P_{eB}(PO, 4, N, P_{eb})$ was not carried out, and it is clear that the determination and computation of the exact formula for $P_{eB}(PO, M, N, P_{eb})$ when $M > 4$ is not feasible.

Determination of P_{eB} by Simulation

Since we could not determine $P_{eB}(ERO, M, N, P_{eb})$ by exact analytic methods for $M > 4$, and since the same is true for $P_{eB}(PO, M, N, P_{eb})$ when $M > 4$, we next considered simulation of our M-ary communication system on the digital computer in order to derive estimates for P_{eB} in either the ERO or PO case. A description of the simulation program is given in App. D.

Let us consider the estimation of $P_{eB}(ERO, M, N, P_{eb})$ using simulation. If we fix M, then the parameters affecting the simulation results are P_{eb}, N, and the number of times n that the simulation program is repeated. If we generate n error blocks each having N bits, with the probability of a bit error $[P(1)]$ equal to P_{eb}, then we would theoretically expect $K_N(n) = n\binom{N}{K}P_{eb}^K\, Q_{eb}^{N-K}$ error blocks to have K bit errors. Due to the characteristics of a particular random-number-generator algorithm, we find experimentally that, although these theoretical values are rarely met in practice, if we apply a χ^2 goodness of fit test to the observed and theoretical values, then we would accept the hypothesis that the computer is giving us a probability of bit error equal to P_{eb}.

In order that the relative frequency of a block error should approach $P_{eB}(ERO, M, N, P_{eb})$, we must have n large enough so that, over the range where K bit errors can influence the block error count, $K_N(n)$ is nonzero. This assures that a sufficient number of useful samples exists to make the results of the simulation meaningful. We might conclude immediately that $K_N(n)$ should be nonzero for $N/4 \le K \le N$. Due to the dependency relations caused by any M-ary ERO block code, we can replace the upper limit of N on K by a smaller upper limit since beyond this limit the probability of a block error will necessarily be equal to one. For $M = 3$, this upper limit becomes $(3N/4)-2$, and for $M = 4$ the upper limit is $(5N/8)-1$. If it is possible to make $K_N(n)$ nonzero over this restricted range, then the simulation answer can be taken as the relative frequency of error. The term representing the probability of a block error for $N \ge K \ge$ upper limit + 1, which is given by

$$\sum_{k=\text{upper limit}+1}^{N}\binom{N}{K}P_{eb}^K\, Q_{eb}^{N-K},$$

may be added to the relative frequency measure to give a better approximation to P_{eB}(ERO, M, N, P_{eb}). If n is sufficiently large and $P_{eb} \geq 0.30$, then the simulation-derived relative frequency measure is quite close to P_{eB}(ERO, M, N, P_{eb}) since $K_N(n)$ is nonzero over more than just the restricted range, and hence the additional term is not necessary and, in fact, is usually redundant as far as the error count is concerned.

The choice of n in practice was governed by the ability to cover as much of the range of significant values as possible without making the run time of the simulation program too long, yet allowing enough trials so that the relative frequency would approximate P_{eB}(ERO, M, N, P_{eb}) within an accuracy of 2%. We decided to set $n = 10,000$ since this value was consistent with our computational time objective and also allowed a relative frequency approximation to be significant for P_{eB}(ERO, M, N, P_{eb}) ≥ 0.01. Since we always have the relation that P_{eB}(ERO, $2, N, P_{eB}$) < P_{eB} (ERO, M, N, P_{eb}) for $M \geq 3$, and since we know all the values for P_{eB}(ERO, $2, N, P_{eb}$), we can, given M and N, choose P_{eb} so that P_{eB} (ERO, $2, N, P_{eb}$) ≥ 0.01, and hence so that P_{eB}(ERO, M, N, P_{eb}) ≥ 0.01.

Table 7 shows results of the simulation when $M = 4$ for $n = 10,000$ trials per simulation run given various values of N and P_{eb}. The examples given in Table 7 show clearly the interplay between n, N, and P_{eb}. As an example of the effect of increasing n, if we had set $n = 30,000$ and computed the relative frequency for $N = 8$ and $P_{eb} = 0.05$, then the result of simulating P_{eB} would be 3.15×10^{-2}, with a run time of 25 sec. For small values of N, we can increase n to gain accuracy without greatly increasing the run time of the simulation program. For large values of N, accuracy and run time are in direct competition, such that a greatly increased run time will result in only a slight gain in accuracy. For small increases in M, the run time may not change significantly since the upper limit on K decreases as M increases, and therefore fewer of these increased length correlation decision procedures will be performed.

Now let us consider the estimation of P_{eB} (PO, M, N, P_{eb}) using simulation. The factors affecting the simulation results are M, N, P_{eb}, n, and the generation of the PO block code for M and N.

Let us assume that the problem concerning the time it takes to generate the PO block code has been taken care of, we then examine the effects of the remaining parameters.

Given n, we would theoretically expect $\bar{n}(d_{min}) = n \times P(d_{min}, M, N)$, iterations to have a PO block code with minimum distance d_{min}. If we apply a χ^2 goodness-of-fit test to the observed and theoretical values of $\bar{n}(d_{min})$, then we would accept the hypothesis that we have indeed generated PO block codes with $P(b_{ij} = 1) = P(b_{ij} = 0) = 1/2$ ($i = 1, \ldots, M$; $j = 1, \ldots, N$). In order that the relative frequency of a block error should approach P_{eB} (PO, M, N, P_{eb}), the observed values of $\bar{n}(d_{min})$ must be nonzero over the range of d_{min} which can influence the error count. The worst problem here occurs when P_{eb} is small, and hence the small values of d_{min} exert the most influence on the error count, but these values of d_{min} are usually such that $\bar{n}(d_{min})$ is zero unless M is very large, possibly on the order of twice the value of N.

Unlike the ERO case, we must carry out the correlation operation for each iteration. This adds greatly to the run time. The larger that M and N are, the larger is the increase in run time.

Now let us consider the problem of the time required to generate the PO block code. The CDC 3800 computer located at NRL generates a real-valued uniform random number on $[0,1]$ in 34×10^{-6} sec. For each iteration we need $M \times N$ such numbers to determine the PO code. Hence, it takes $34 \times M \times N \times 10^{-6}$ sec to generate a PO block code. Since this must be done for each iteration, then for $n = 10^4$ iterations we find that it takes $0.34 \times M \times N$ sec for the simulation program to generate the desired PO block codes.

Table 7
Comparison of Simulated (Approximate) P_{eB} Values with Analytical (Exact) Values for an ERO Block Code with $M=4$. The Number of Trials n for Each Simulation Run was 10,000.

N	P_{eb}	$P_{eB}(ERO, 4, N, P_{eb})$ Simulated	Analytical	Computer Time (sec)
8	0.2	$3.47*10^{-1}$	$3.414*10^{-1}$	19
8	0.1	$1.12*10^{-1}$	$1.136*10^{-1}$	20
8	0.05	$2.98*10^{-2}$	$3.267*10^{-2}$	20
16	0.2	$1.33*10^{-1}$	$1.282*10^{-1}$	24
16	0.15	$5.57*10^{-2}$	$5.255*10^{-2}$	23
16	0.1	$1.37*10^{-2}$	$1.326*10^{-2}$	22
16	0.05	$.9*10^{-4}$	$1.044*10^{-3}$	21
32	0.45	$6.82*10^{-1}$	$6.858*10^{-1}$	46
32	0.20	$1.83*10^{-2}$	$1.86*10^{-2}$	33
32	0.15	$2.3*10^{-3}$	$2.976*10^{-3}$	28
64	0.35	$1.36*10^{-1}$	$1.342*10^{-1}$	79
64	0.30	$3.74*10^{-2}$	$3.584*10^{-2}$	71
128	0.40	$1.58*10^{-1}$	$1.537*10^{-1}$	139
128	0.35	$2.7*10^{-2}$	$2.547*10^{-2}$	141

As an example of how many seconds are involved, the following table lists values of $0.34 \times M \times N$ for several M and N.

N \ M	3	16	64
64	65.28 sec	348.16 sec	1,392.64 sec
1024	704.48 sec	5570.56 sec	22,282.24 sec

Clearly, except for small values of $M \times N$, the time involved in the generation of the PO block codes restricts the use of simulation in determining $P_{eB}(PO, M, N, P_{eb})$.

The problems associated with the simulation of P_{eB} (ERO or PO, M, N, P_{eb}) as outlined above leave us with two main avenues of approach. The first approach involves an investigation of the use of assembly language programming in order to decrease the required run time of the simulation program. The second approach involves an investigation of the use of a special-purpose statistical device. Such a device becomes extremely useful when attempts to circumvent the problem of excessive run times are not successful, since its use is not limited by the cost of long run times as is the case for general-purpose computers. Thus, a special purpose statistical device can allow us to accommodate large values of M and N and small values of P_{eb} in computing P_{eB}(ERO or PO, M, N, P_{eb}). We will examine these approaches as part of our continuing research into these problems.

If we compare the $P_{eB}(ERO, 2, N, P_{eb})$ and $P_{eB}(PO, 2, N, P_{eb})$ curves, or the $P_{eB}(ERO, 3, N, P_{eB})$ and $P_{eB}(ERO, 3, N, P_{eb})$ curves, we notice that for high P_{eb} values, i.e., P_{eb} close to 1/2, the PO curves surprisingly have a lower probability of block error than the corresponding ERO curves (i.e., for the same values of M and N). For low values of P_{eb}, i.e., P_{eb} less than 10^{-3}, the ERO curves have a lower probability of a block error than the corresponding PO curves. This is due to the fact that the ERO curves tend to zero as P_{eb} tends to zero, whereas the PO curves tend to their respective nonzero asymptotic values as P_{eb} tends to zero. The exact values of P_{eb} for which the above relationships hold depends on the values of M and N.

AREAS FOR FURTHER INVESTIGATION

In the course of carrying out this research, we have examined closely M-ary communication employing a bit-by-bit decision techniques. As an area of further investigation we intend to examine the use of block decision techniques. The techniques to be employed were outlined and examined for certain binary block codes(1). This is a natural extension of this work due to the processing gain inherent in the use of block decision techniques. The use of block decisions is extremely important because of the fact that with block decisions the representation of P_{eB} in terms of an exact formula capable of being easily computed for all values of M and N seems to be possible.

REFERENCE

1. Balthasar, N. C., and Beck, H. M., "Digital Receiver Decision Techniques for Certain Fixed Length Binary Block Codes Transmitted Through the Gaussian Channel," NRL Report, 7014, Nov. 1969.

APPENDIX A

GENERATING M-ARY ERO AND M-ARY PO BLOCK CODES

In this Appendix, we will describe some methods of generating M-ary ERO and M-ary PO block codes.

Let us consider first the generation of M-ary ERO block codes. An M-ary ERO block code can be derived by utilizing a device which can generate the Walsh functions of order N (A1, A2). The Walsh functions of order N are N time functions taking on the value 0 or 1 over each of N time periods of length t(t = bit time) such that, except for the all zeros Walsh function, each function has $N/2$ zeros and $N/2$ ones, and the correlation between any two functions is zero. Thus, by removing the all zeros Walsh function, the remaining functions form an $M = N-1$ ERO block code.

Another method of deriving an M-ary ERO block code uses maximal length linear shift register sequences (A3). If $N = 2^K$, then we know that there is a maximal length linear shift register sequence of length 2^K-1. From the properties of such a sequence, we know that if we add a zero to the sequence and each of its 2^K-2 cyclic shifts, then these form an $M = 2^K-1$ ERO block code.

Now let us consider the generation of M-ary PO block codes. One method of deriving an M-ary PO block code utilizes a random number generator which generates MN real numbers u_{ij} ($i = 1, 2, \ldots, M$ and $j = 1, 2, \ldots, N$) having a uniform distribution over the interval $[0, 1]$. Given such a random number generator, which can be found as a library function in most large computers, if we set $b_{ij} = 0$ when $0 \le u_{ij} < 1/2$, and $b_{ij} = 1$ when $1/2 \le u_{ij} \le 1$, then the resulting M by N matrix $B = [b_{ij}]$ forms an M-ary PO block code. There are many available methods of generating real numbers having a uniform distribution on $[0,1]$ (A4). Another method of deriving an M-ary PO block code involves the outcome of M trials each consisting of N tossings of an unbiased coin (i. e., P(head) = P(tail) = 1/2). From the MN outcomes of tossing the unbiased coin we form MN binary numbers b_{ij} ($i = 1, 2, \ldots M$ and $j = 1, 2, \ldots, N$) where $b_{ij} = 0$ if the jth outcome of the ith trial is a head, and $b_{ij} = 1$ if it is a tail. Clearly, the resulting matrix $B = [b_{ij}]$ forms an M-ary PO block code.

In attempting to generate an M-ary PO block code, one must consider the effect of the inherent bias found in any generation method. Suppose that instead of having $P(b_{ik} = 0) = P(b_{ik} = 1) = 1/2$ ($i = 1, 2, \ldots, M$ and $k = 1, 2, \ldots, N$) due to a bias, we actually have $P(b_{ik} = 0) = 1/2+\epsilon$ and $P(b_{ik} = 1) = 1/2-\epsilon$. In this case, N_{xi} and N_{yi} (the number of zeros and ones, respectively, in block B_i) are random variables having binomial distributions $B(n, p)$ with $n = N$ and $p = 1/2 + \epsilon$ and $p = 1/2 - \epsilon$, respectively. Thus, D_{ij} (the number of disagreements between blocks B_i and B_j) is a random variable having a binomial distribution $B(n,p)$ with $n = N$ and $p = 1/2 - 2\epsilon^2$. Thus, a bias causes the M PO blocks to become more alike. This decreases the ability of the code to resist errors, and hence increases the probability of a block error.

REFERENCES

A1. Andrews, D. C., and Beck, H. M., "The Synthesis of Biorthogonal Time-Reversible Walsh-Hadamard Functions," NRL Progress Report, April 1970.

A2. Lee, J. S., "Generation of Walsh Functions as Binary Group Codes," Proceedings of 1970 Symposium on Applications of Walsh Functions, Naval Research Laboratory, March 31 - April 3, 1970.

A3. Golomb, S. W., "Introduction to Digital Communication," (Sect. 1.4) in "Digital Communications with Space Applications," New Jersey: Prentice-Hall, 1964.

A4. Hull, T. E., and Dobell, A. R., "Random Number Generators," SIAM Rev. 4 (No. 3), July 1962.

APPENDIX B

DERIVATION OF P_{eB} FORMULAS FOR TERNARY ERO AND PO BLOCK CODES

In this Appendix we derive the probability of block error formulas for ternary ERO and PO block codes.

Let $B = \{B_1, B_2, B_3\}$ denote a ternary ERO block code, and suppose that B_1 is the transmitted block. If N_{123}, N_{12}, N_{13}, and N_{23} represent the number of bits k such that $b_{1k} = b_{2k} = b_{3k}$, $(b_{1k} = b_{2k}) \neq b_{3k}$, $(b_{1k} = b_{3k}) \neq b_{2k}$, and $(b_{2k} = b_{3k}) \neq b_{1k}$, respectively, then from the properties of ERO blocks we have, assuming that $N/4$ is an integer, $N_{123} = N_{12} = N_{13} = N_{23} = N/4$. The $N/4$ bits denoted by N_{123} do not influence the probability of a block error since a bit decision error with respect to any of these bits does not affect the correlation decision. Hence, we must consider the remaining $3N/4$ bits in determining P_{eB}. If e_{23}, e_{13}, and e_{12} represent the number of bit errors in the N_{23}, N_{13}, and N_{12} groups of bits, respectively, then a block error occurs if

(i) $e_{23} < N/4$ (and $e_{23} + e_{12} \geq N/4$, or $e_{23} + e_{13} \geq N/4$)

or

(ii) $e_{23} = N/4$.

Hence,

$$P_{eB}(ERO,3,N,P_{eb}) = \sum_{J=0}^{(N/4)-1} \binom{N/4}{J} P_{eb}^{J} Q_{eb}^{(N/4)-J} \left\{ \sum_{K=(N/4)-J}^{N/4} \binom{N/4}{K} P_{eb}^{K} Q_{eb}^{(N/4)-K} \left[1 + \sum_{L=0}^{(N/4)-J-1} \binom{N/4}{L} P_{eb}^{L} Q_{eb}^{(N/4)-L} \right] \right\} + P_{eb}^{N/4}.$$

Next, let $B = \{B_1, B_2, B_3\}$ denote a ternary PO block code, and suppose that B_1 is the transmitted block. If D_{ij} denotes the number of bit disagreements between blocks B_i and B_j, then from the properties of PO blocks given above we know that D_{12} and D_{13} are independent binomially distributed random variables $B(n,p)$ with parameters $n = N$ and $p = 1/2$. Hence, the joint probability of D_{12} and D_{13} is given by

$$P(D_{12}, D_{13}) = P(D_{12})\,P(D_{13}) = \left[\frac{\binom{N}{D_{12}}}{2^N} \right] \left[\frac{\binom{N}{D_{13}}}{2^N} \right] \quad (D_{12}, D_{13} = 0, 1, \ldots, N).$$

Let d_{min} and d_{max} equal the minimum and maximum of D_{12} and D_{13}, respectively. Let d_0 equal the number of bits k such that $b_{1k} \neq (b_{2k} = b_{3k})$. Clearly, $0 \leq d_0 \leq d_{min}$. The number of bits k such that $(b_{1k} \neq b_{3k}) = b_{2k}$ is $D_{12} - d_0$, and the number of bits k such that $(b_{1k} = b_{2k}) \neq b_{3k}$ is $D_{13} - d_0$. Given D_{12} and D_{13}, or equivalently d_{min} and d_{max}, the probability distribution of d_0 is given by

$$P(d_0) = \frac{\binom{d_{min}}{d_0} \binom{N - d_{min}}{d_{max} - d_0}}{\binom{N}{d_{max}}} \quad (d_0 = 0, 1, \ldots, d_{min}).$$

It is easy to show that

$$\sum_{d_0=0}^{d_{min}} P(d_0) = 1 \quad (d_{min} = 0, 1, \ldots, N).$$

Let e_1, e_2, and e_3 denote the number of errors in the bits where $b_{1k} \neq (b_{2k} = b_{3k})$, $(b_{1k} = b_{3k}) \neq b_{2k}$, and $(b_{1k} = b_{2k}) \neq b_{3k}$, respectively. Clearly, from the above we have $0 \le e_1 \le d_0$, $0 \le e_2 \le D_{12} - d_0$, and $0 \le e_3 \le D_{13} - d_0$. Let

$$d_i = \begin{Bmatrix} d_{min}/2, & (d_{min} \text{ even}) \\ (d_{min}+1)/2, & (d_{min} \text{ odd}) \end{Bmatrix} \text{ and } d_x = \begin{Bmatrix} d_{max}/2, & (d_{max} \text{ even}) \\ (d_{max}+1)/2, & (d_{max} \text{ odd}) \end{Bmatrix}.$$

Now given D_{12}, D_{13}, and d_0, a block error occurs when

$$\text{(i)} \quad e_1 < d_i, \text{ and } \begin{Bmatrix} e_1 + e_2 \ge d_i, \text{ or } e_1 + e_3 \ge d_x;\ d_{min} = D_{12} \text{ and } d_{max} = D_{13} \\ e_1 + e_3 \ge d_i, \text{ or } e_1 + e_2 \ge d_x;\ d_{min} = D_{13} \text{ and } d_{max} = D_{12} \end{Bmatrix},$$

or

$$\text{(ii)} \quad e_1 \ge d_i.$$

Hence

$$P_{eB}(P0, 3, N, P_{eb}) = \sum_{D_{12}=0}^{N} \sum_{D_{13}=0}^{N} \left(\frac{\binom{N}{D_{12}}\binom{N}{D_{13}}}{2^{2N}} \right) \left[\sum_{d_0=0}^{d_{min}} \left(\frac{\binom{d_{min}}{d_0}\binom{N-d_{min}}{d_{max}-d_0}}{\binom{N}{d_{max}}} \right) R \right]$$

where

$$R = \sum_{e=0}^{d_i-1} \binom{d_0}{e} P_{eb}^{e} Q_{eb}^{d_0-e} \left\{ \sum_{J=d_i-e}^{d_{min}-d_0} \binom{d_{min}-d_0}{J} P_{eb}^{J} Q_{eb}^{d_{min}-d_0-J} + \left[\left(\sum_{k=0}^{d_i-e-1} \binom{d_{min}-d_0}{K} P_{eb}^{K} Q_{eb}^{d_{min}-d_0-K} \right) T \right] \right\}$$

$$+ \sum_{e=d_i}^{d_0} \binom{d_0}{e} P_{eb}^{e} Q_{eb}^{d_0-e} \text{ with } T = \sum_{L=d_x-e}^{d_x-d_0} \binom{d_{max}-d_0}{L} P_{eb}^{L} Q_{eb}^{d_{max}-d_0-L}.$$

If we combine the terms of $P_{eB}(P0, 3, N, P_{eb})$ when $D_{12} = 0$, $D_{13} = 0$, or both D_{12} and $D_{13} = 0$, then, since for all these terms we have $R = 1$ and $d_{min} = 0$, the resulting term is $(2^{N+1} - 1)/2^{2N}$ which is easily seen to be the value of $P(d_{min} = 0, 3, N)$. Thus, we can rewrite the above as

$$P_{eB}(P0, 3, N, P_{eb}) = \sum_{D_{12}=1}^{N} \sum_{D_{13}=1}^{N} \frac{\binom{N}{D_{12}}\binom{N}{D_{13}}}{2^{2N}} \left[\sum_{d_0=0}^{d_{min}} \left(\frac{\binom{d_{min}}{d_0}\binom{N-d_{min}}{d_{max}-d_0}}{\binom{N}{d_{max}}} \right) R \right] + \frac{(2^{N+1}-1)}{2^{2N}}.$$

It is readily apparent that this equation due to its complicated nature is lengthy to compute. The equation in this form was computed on the CDC 3800 for $N = 4$, 8, and 16. The total time required to compute these curves was approximately 2 min. The estimated time required to compute the curve for $N = 32$ was 10 min. Due to this lengthy computation time estimate, methods of approximating the above equation were investigated. Instead of using the double sum over D_{12} and D_{13}, this was replaced by a single sum using $P(d_{min}, M, N)$ rather than $P(D_{12})$ and $P(D_{13})$. Hence, one needed only to sum over d_{min} from 1 to N. But this introduced the problem that d_{max} was no longer defined explicity. It was found that if d_{max} was determined in terms of d_{min} using an algorithm which set d_{max} equal to d_{min} plus the smallest integer greater than or equal to $(N - d_{min})/(N/4)$, then the approximation was within 1% of the true value. As a further approximation, an algorithm was employed to determine d_0 given d_{min} and d_{max} and thus avoid the summing of d_0 from zero to d_{min}. This algorithm set $d_0 = d_i$ if $d_{min} + d_{max} - N \le d_i$, and set $d_0 = d_{min} = d_{max} - N$ if $d_{min} + d_{max} - N > d_i$. This algorithm chose the most likely nonzero value of d_0 consistent with the $P(d_0)$ distribution. It was found that this additional approximation introduced no significant change in the approximation to $P_{eB}(PO, 3, N, P_{eb})$. The P_{eB} curves for $N = 32$, 64, and 128 were computed using these approximations. Despite the utilization of these approximations, it took almost 9 min to compute P_{eB} for the case where $N = 128$. Hence, this was the largest value of N which was computed for $P_{eB}(PO, 3, N, P_{eb})$.

If we consider an ϵ bias, then $P_{eB}(PO, \epsilon(\text{bias}), 3, N, P_{eb})$ differs from $P_{eB}(PO, 3, N, P_{eb})$ only in that $P(D_{12}, D_{13})$ becomes

$$P(D_{12}, D_{13}) = \binom{N}{D_{12}}\binom{N}{D_{13}} [(1/2) - 2\epsilon^2]^{(D_{12}+D_{13})} [(1/2) + 2\epsilon^2]^{N-(D_{12}+D_{13})}.$$

APPENDIX C

DERIVATION OF P_{eB} FORMULA FOR QUATERNARY ERO BLOCK CODES

In this Appendix we consider the derivation of $P_{eB}(ERO, 4, N, P_{eb})$.

Let $B = \{B_1, B_2, B_3, B_4\}$ denote a quaternary ERO block code, and suppose B_1 is the transmitted block. If N_0, N_1, N_{12}, N_{13}, N_{14}, N_{123}, N_{124}, and N_{134} represent the number of bits k such that $b_{1k} = b_{2k} = b_{3k} = b_{4k}$, $b_{1k} \neq (b_{2k} = b_{3k} = b_{4k})$, $(b_{1k} = b_{2k}) \neq (b_{3k} = b_{4k})$, $(b_{1k} = b_{3k}) \neq (b_{2k} = b_{4k})$, $(b_{1k} = b_{4k}) \neq (b_{2k} = b_{3k})$, $b_{4k} \neq (b_{1k} = b_{2k} = b_{3k})$, $b_{3k} \neq (b_{1k} = b_{2k} = b_{4k})$ and $b_{2k} \neq (b_{1k} = b_{3k} = b_{4k})$, respectively, then from the properties of ERO blocks we have, assuming that $N/8$ is an integer, $N_0 = N_1 = N_2 = N_{13} = N_{14} = N_{123} = N_{124} = N_{134} = N/8$. The $N/8$ bits denoted by N_0 do not influence the probability of a block error since a bit decision error with respect to any of these bits does not affect the correlation decision. Hence, we must consider the remaining $7N/8$ bits in determining P_{eB}. If e_1, e_{12}, e_{13}, e_{14}, e_{123}, e_{124}, and e_{134} represent the number of bit errors in the N_1, N_{12}, N_{13}, N_{14}, N_{123}, N_{124}, and N_{134} groups of bits, respectively, then a block error occurs if

(i) $e_1 + e_{13} + e_{14} + e_{134} \geq N/4$

or

(ii) $e_1 + e_{12} + e_{14} + e_{124} \geq N/4$

or

(iii) $e_1 + e_{12} + e_{13} + e_{123} \geq N/4$.

Hence,

$$P_{eB}(ERO, 4, N, P_{eb}) = \sum_{e_1=0}^{N/8} \sum_{e_{12}=0}^{N/8} \sum_{e_{13}=0}^{N/8} \sum_{e_{14}=0}^{N/8} \binom{N/8}{e_1}\binom{N/8}{e_{12}}\binom{N/8}{e_{13}}\binom{N/8}{e_{14}} P_{eb}^{(e_1+e_{12}+e_{13}+e_{14})} Q_{eb}^{(N/2)-(e_1+e_{12}+e_{13}+e_{14})} R$$

where

$$R = \begin{cases} 1, \text{ if } e_1 + e_{13} + e_{14} \geq N/4, \text{ or } e_1 + e_{12} + e_{14} \geq N/4, \text{ or } e_1 + e_{12} + e_{13} \geq N/4 \\ T, \text{ otherwise} \end{cases}.$$

Here

$$T = A + (1-A)\,B + (1-A)\,(1-B)\,C$$

where

$$A = \sum_{e_{134}=(N/4)-(e_1+e_{13}+e_{14})}^{N/8} \binom{N/8}{e_{134}} P_{eb}^{e_{134}} Q_{eb}^{(N/8)-e_{134}},$$

$$B = \sum_{e_{124}=(N/4)-(e_1+e_{12}+e_{14})}^{N/8} \binom{N/8}{e_{124}} P_{eb}^{e_{124}} Q_{eb}^{(N/8)-e_{124}},$$

and

$$C = \sum_{e_{123}=(N/4)-(e_1+e_{12}+e_{13})}^{N/8} \binom{N/8}{e_{123}} P_{eb}^{e_{123}} Q_{eb}^{(N/8)-e_{123}}.$$

This equation was programmed directly on the CDC 3800 located at NRL and gave P_{eB} (ERO, 4, N, P_{eb}), using various values of P_{eb} for N up to 128, without experiencing any computational difficulties. When the case N = 256 was tried, the run time increased so drastically that it became quite apparent that, in order to compute P_{eB}(ERO, 4, 256, P_{eb}), some method of approximation would have to be employed. The fourfold summation process involved in the exact formula constituted the major computational difficulty. For N = 64 and N = 128, the summation process involved 6561 and 83, 521 iterations, respectively. From the run times for these values of N, it was estimated that each iteration took approximately 1.5 msec. Since the case N = 256 involved 1, 185, 921 iterations, the estimated run time was approximately 30 min. The estimated run time for the case N = 512 was found to be 8 hr.

Now we can replace the fourfold summation from zero to N/2. But given e errors, where $0 \le e \le N/2$, we must then choose particular values of e_1, e_{12}, e_{13}, and e_{14}, say e_1^*, e_{12}^*, e_{13}^*, and e_{14}^*, such that $e_1^*+e_{12}^*+e_{13}^*+e_{14}^* = e$, and

$$\binom{N/2}{e} P_{eb}^{e} Q_{eb}^{(N/2)-e} P_{eB}\Big|_{e_1^*, e_{12}^*, e_{13}^*, e_{14}^*} \simeq \underset{\substack{\text{(such that } e_1+e_{12}\\ +e_{13}+e_{14}=e)}}{\sum_{e_1}\sum_{e_{12}}\sum_{e_{13}}\sum_{e_{14}}} \binom{N/8}{e_1}\binom{N/8}{e_{12}}\binom{N/8}{e_{13}}\binom{N/8}{e_{14}} S$$

where

$$S = P_{eb}^{e} Q_{eb}^{(N/2)-e} P_{eb}\Big|_{e_1, e_{12}, e_{13}, e_{14}}.$$

Upon attempting to carry out this scheme of approximation, it was found that the choice of e_1^*, e_{12}^*, e_{13}^*, and e_{14}^* was dependent on P_{eb} and e. This made the approximation as difficult to carry out as the exact formula. Due to these factors, the case N = 128 was chosen as a stopping point for the computation of P_{eB}(ERO, 4, N, P_{eb}).

APPENDIX D

DESCRIPTION OF THE DIGITAL COMPUTER SIMULATION OF THE M-ARY COMMUNICATION SYSTEM

In this Appendix we describe the digital computer simulation of our M-ary communication system.

To initiate the simulation we must generate and/or store the M by N matrix for an M-ary ERO or PO block code. In the case of an M-ary ERO block code, we can simply enter the M blocks of N bits as data into core storage. In the case of an M-ary PO block code, we can use the random number generator technique described in App. A to generate the desired PO matrix. For the PO case, we will have to generate a new M by N matrix for each iteration of the basic program.

The choice of a block to be transmitted can, without loss of generality, be made in a deterministic manner and held constant over all iterations. The use of digital simulation allows us to bypass the transmitter and receiver portions of the system.

To simulate the channel's action on the transmitted block we generate an error block $e = [e_1, \ldots, e_N]$ using the random number generator such that $P(e_i = 1) = P_{eb}$, the probability of a bit error. To do this we generate, using the random number generator, real numbers $u_1, \ldots, u_N$ having a uniform distribution on $[0,1]$ and we set $e_i = 1$ if $0 \leq u_i \leq P_{eb}$, and $e_i = 0$ if $P_{eb} < u_i < 1$. Now by adding modulo two the transmitted block and the error block, term by term, the block of bit decisions D results.

Next we perform the matrix operations necessary to compute $\rho_1, \ldots, \rho_M$. Now using the fact that the transmitted block can be chosen deterministically, and this choice is the same for all iterations, it is quite simple to test the values $\rho_1, \ldots, \rho_M$ for an error.

Finally, we need only record the errors and, after repeating the desired number of iterations, determine the relative frequency of a block error.

The simulation as described above was implemented in FORTRAN computer language.